From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Commissioner
US Department of Commerce
United States Patent and Trademark Office, PCT
2011 South Clark Place Room CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 12 January 2001 (12.01.01)	
International application No. PCT/FI00/00353	**Applicant's or agent's file reference** 49705
International filing date (day/month/year) 25 April 2000 (25.04.00)	**Priority date** (day/month/year) 26 April 1999 (26.04.99)
Applicant HAUMONT, Serge	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

26 November 2000 (26.11.00)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer R. E. Stoffel
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

Form PCT/IB/331 (July 1992)

FI0000353

The demand must be filed direc[redacted]th the competent International Preliminary Examining Authority or, if two or more Authorities are competent, with the one chosen by the appl[redacted] The full name or two-letter code of that Authority [redacted]e indicated by the applicant on the line below:

IPEA/ EPO

[redacted]

PCT

CHAPTER II

DEMAND

under Article 31 of the Patent Cooperation Treaty:
The undersigned requests that the international application specified below be the subject of international preliminary examination according to the Patent Cooperation Treaty and hereby elects all eligible States (except where otherwise indicated).

For International Preliminary Examining Authority use only

Identification of IPEA	Date of receipt of DEMAND

Box No. I IDENTIFICATION OF THE INTERNATIONAL APPLICATION

Applicant's or agent's file reference: 49705/ML/MM

International application No.	International filing date *(day/month/year)*	(Earliest) Priority date *(day/month/year)*
PCT/FI00/00353	25 April 2000 (25.4.00)	26 April 1999 (26.4.99)

Title of invention: NEW METHOD FOR CHECKING THE DATA

Box No. II APPLICANT(S)

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

NOKIA NETWORKS OY
P.O.Box 300
FIN-00045 NOKIA GROUP
Finland

Telephone No.:

Facsimile No.:

Teleprinter No.:

State *(that is, country)* of nationality:	State *(that is, country)* of residence:
Finland	Finland

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

HAUMONT, Serge
Riistavuorenkuja 3 B 10
FIN-00320 HELSINKI
Finland

State *(that is, country)* of nationality:	State *(that is, country)* of residence:
France	Finland

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

State *(that is, country)* of nationality:	State *(that is, country)* of residence:

☐ Further applicants are indicated on a continuation sheet.

International application No.
PCT/FI00/00353

Box No. III AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE

The following person is [x] agent [ ] common representative

and [x] has been appointed earlier and represents the applicant(s) also for international preliminary examination.

[ ] is hereby appointed and any earlier appointment of (an) agent(s)/common representative is hereby revoked.

[ ] is hereby appointed, specifically for the procedure before the International Preliminary Examining Authority, in addition to the agent(s)/common representative appointed earlier.

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

BERGGREN OY AB
P.O. Box 16
FIN-00101 HELSINKI
Finland

Telephone No.: +358-9-693701

Facsimile No.: +358-9-6933944

Teleprinter No.:

[ ] **Address for correspondence:** Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special addr ess to which correspondence should be sent.

Box No. IV BASIS FOR INTERNATIONAL PRELIMINARY EXAMINATION

Statement concerning amendments:*

1. The applicant wishes the international preliminary examination **to start on the basis of:**

[x] the international application as originally filed

the description [x] as originally filed
[ ] as amended under Article 34

the claims [x] as originally filed
[ ] as amended under Article 19 (together with any accompanying statement)
[ ] as amended under Article 34

the drawings [x] as originally filed
[ ] as amended under Article 34

2. [ ] The applicant wishes any amendment to the claims under Article 19 to be considered as reversed.

3. [ ] The applicant wishes the start of the international preliminary examination **to be postponed** until the expiration of 20 months from the priority date unless the International Preliminary Examining Authority receives a copy of any amendments made under Article 19 or a notice from the applicant that he does not wish to make such amendments (Rule 69.1(d)). *(This check-box may be marked only where the time limit under Article 19 has not yet expired.)*

* Where no check-box is marked, international preliminary examination will start on the basis of the international application as originally filed or, where a copy of amendments to the claims under Article 19 and/or amendments of the international application under Article 34 are received by the International Preliminary Examining Authority before it has begun to draw up a written opinion or the international preliminary examination report, as so amended.

Language for the purposes of international preliminary examination: English

[x] which is the language in which the international application was filed.
[ ] which is the language of a translation furnished for the purposes of international search.
[x] which is the language of publication of the international application.
[ ] which is the language of the translation (to be) furnished for the purposes of international preliminary examination.

Box No. V ELECTION OF STATES

The applicant hereby **elects all eligible States** *(that is, all States which have been designated and which are bound by Chapter II of the PCT)*

excluding the following States which the applicant wishes **not to elect:**

International application No.
PCT/FI00/00353

Box No. VI CHECK LIST

The demand is accompanied by the following elements, in the language referred to in Box No. IV, for the purposes of international preliminary examination:			For International Preliminary Examining Authority use only: received	not received
1. translation of international application	:	sheets	☐	☐
2. amendments under Article 34	:	sheets	☐	☐
3. copy (or, where required, translation) of amendments under Article 19	:	sheets	☐	☐
4. copy (or, where required, translation) of statement under Article 19	:	sheets	☐	☐
5. letter	:	sheets	☐	☐
6. other *(specify)*	:	sheets	☐	☐

The demand is also accompanied by the item(s) marked below:

1. [X] fee calculation sheet
2. [ ] separate signed power of attorney
3. [ ] copy of general power of attorney; reference number, if any:
4. [ ] statement explaining lack of signature
5. [ ] nucleotide and or amino acid sequence listing in computer readable form
6. [ ] other *(specify)*:

Box No. VII SIGNATURE OF APPLICANT, AGENT OR COMMON REPRESENTATIVE

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the demand).

BERGGREN OY AB

Juhani Kupiainen
Patent Agent

26 November 2000

For International Preliminary Examining Authority use only

1. Date of actual receipt of DEMAND:
2. Adjusted date of receipt of demand due to CORRECTIONS under Rule 60.1(b):
3. ☐ The date of receipt of the demand is AFTER the expiration of 19 months from the priority date and item 4 or 5, below, does not apply. ☐ The applicant has been informed accordingly.
4. ☐ The date of receipt of the demand is WITHIN the period of 19 months from the priority date as extended by virtue of Rule 80.5.
5. ☐ Although the date of receipt of the demand is after the expiration of 19 months from the priority date, the delay in arrival is EXCUSED pursuant to Rule 82.

For International Bureau use only

Demand received from IPEA on:

See Notes to the demand form

CHAPTER II

PCT

FEE CALCULATION SHEET

Annex to the Demand for international preliminary examination

International application No.	PCT/FI00/00353
Applicant's or agent's file reference	49705/ML/MM

For International Preliminary Examining Authority use only

Date stamp of the IPEA

Applicant

NOKIA NETWORKS OY

Calculation of prescribed fees

1. Preliminary examination fee	EUR 1533	P
2. Handling fee *(Applicants from certain States are entitled to a reduction of 75% of the handling fee. Where the applicant is (or all applicants are) so entitled, the amount to be entered at H is 25% of the handling fee.)*	EUR 147	H
3. Total of prescribed fees Add the amounts entered at P and H and enter total in the TOTAL box.....	EUR 1680	TOTAL

Mode of Payment

☐	authorization to charge deposit account with the IPEA (see below)	☐	cash
☐	cheque	☐	revenue stamps
☐	postal money order	☐	coupons
☒	bank draft	☐	other *(specify)*: Bank transfer to account 157230-340380

Deposit Account Authorization *(this mode of payment may not be available at all IPEAs)*

The IPEA/ EPO ☐ is hereby authorized to charge the total fees indicated above to my deposit account.

☐ *(this check-box may be marked only if the conditions for deposit accounts of the IPEA so permit)* is hereby authorized to charge any deficiency or credit any overpayment in the total fees indicated above to my deposit account.

Deposit Account Number | Date *(day/month/year)* | Signature

See Notes to the fee calculation sheet

PCT REQUEST

49705

Original (for **SUBMISSION**) - printed on 25.04.2000 10:40:41 AM

0 0-1	**For receiving Office use only** International Application No.	
0-2	International Filing Date	
0-3	Name of receiving Office and "PCT International Application"	

0-4 0-4-1	**Form - PCT/RO/101 PCT Request** Prepared using	PCT-EASY Version 2.90 (updated 08.03.2000)
0-5	**Petition** The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty	
0-6	**Receiving Office (specified by the applicant)**	National Board of Patents and Registration (Finland) (RO/FI)
0-7	**Applicant's or agent's file reference**	49705
I	**Title of invention**	NEW METHOD FOR CHECKING THE DATA
II II-1 II-2 II-4 II-5 II-6 II-7 II-8 II-9	**Applicant** This person is: Applicant for Name Address: State of nationality State of residence Telephone No. Facsimile No.	applicant only all designated States except US NOKIA NETWORKS OY P.O. Box 300 FIN-00045 Nokia Group Finland FI FI +358-9-51121 +358-9-51168080
III-1 III-1-1 III-1-2 III-1-4 III-1-5 III-1-6 III-1-7	**Applicant and/or inventor** This person is: Applicant for Name (LAST, First) Address: State of nationality State of residence	applicant and inventor US only HAUMONT, Serge Riistavuorenkuja 3 B 10 FIN-00320 Helsinki Finland FR FI

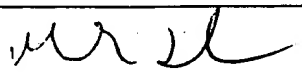
PCT REQUEST 49705

Original (for **SUBMISSION**) - printed on 25.04.2000 10:40:41 AM

IV-1	**Agent or common representative; or address for correspondence** The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:	agent
IV-1-1	Name	BERGGREN OY AB
IV-1-2	Address:	P.O. Box 16 FIN-00101 Helsinki Finland
IV-1-3	Telephone No.	+358-9-693701
IV-1-4	Facsimile No.	+358-9-6933944
IV-1-5	e-mail	email.box@berggren.fi
V	**Designation of States**	
V-1	Regional Patent (other kinds of protection or treatment, if any, are specified between parentheses after the designation(s) concerned)	AP: GH GM KE LS MW SD SL SZ TZ UG ZW and any other State which is a Contracting State of the Harare Protocol and of the PCT EA: AM AZ BY KG KZ MD RU TJ TM and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE and any other State which is a Contracting State of the European Patent Convention and of the PCT OA: BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG and any other State which is a member State of OAPI and a Contracting State of the PCT
V-2	National Patent (other kinds of protection or treatment, if any, are specified between parentheses after the designation(s) concerned)	AE AG AL AM AT AU AZ BA BB BG BR BY CA CH&LI CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW

PCT REQUEST 49705

Original (for **SUBMISSION**) - printed on 25.04.2000 10:40:41 AM

V-5	**Precautionary Designation Statement** In addition to the designations made under items V-1, V-2 and V-3, the applicant also makes under Rule 4.9(b) all designations which would be permitted under the PCT except any designation(s) of the State(s) indicated under item V-6 below. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit.		
V-6	**Exclusion(s) from precautionary designations**	NONE	
VI-1	**Priority claim of earlier national application**		
VI-1-1	Filing date	26 April 1999 (26.04.1999)	
VI-1-2	Number	990936	
VI-1-3	Country	FI	
VI-2	**Priority document request** The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) identified above as item(s):	VI-1	
VII-1	**International Searching Authority Chosen**	European Patent Office (EPO) (ISA/EP)	
VIII	**Check list**	number of sheets	electronic file(s) attached
VIII-1	Request	4	-
VIII-2	Description	11	-
VIII-3	Claims	3	-
VIII-4	Abstract	1	49705.txt
VIII-5	Drawings	4	-
VIII-7	TOTAL	23	
	Accompanying items	paper document(s) attached	electronic file(s) attached
VIII-8	Fee calculation sheet	✓	-
VIII-9	Separate signed power of attorney	✓	-
VIII-10	Copy of general power of attorney	✓	-
VIII-16	PCT-EASY diskette	-	diskette
VIII-18	**Figure of the drawings which should accompany the abstract**	2	
VIII-19	**Language of filing of the international application**	English	
IX-1	**Signature of applicant or agent**		
IX-1-1	Name	BERGGREN OY AB	
IX-1-2	Name of signatory	Markus Levlin	
IX-1-3	Capacity	Patent Agent	

PCT REQUEST

49705

Original (for **SUBMISSION**) - printed on 25.04.2000 10:40:41 AM

FOR RECEIVING OFFICE USE ONLY

10-1	Date of actual receipt of the purported international application	
10-2	Drawings:	
10-2-1	Received	
10-2-2	Not received	
10-3	Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application	
10-4	Date of timely receipt of the required corrections under PCT Article 11(2)	
10-5	International Searching Authority	ISA/EP
10-6	Transmittal of search copy delayed until search fee is paid	

FOR INTERNATIONAL BUREAU USE ONLY

11-1	Date of receipt of the record copy by the International Bureau	

PCT (ANNEX - FEE CALCULATION SHEET)

49705

Original (for **SUBMISSION**) - printed on 25.04.2000 10:40:41 AM

(This sheet is not part of and does not count as a sheet of the international application)

0 0-1	**For receiving Office use only** International Application No.	
0-2	Date stamp of the receiving Office	

0-4 0-4-1	**Form - PCT/RO/101 (Annex)** **PCT Fee Calculation Sheet** Prepared using		PCT-EASY Version 2.90 (updated 08.03.2000)		
0-9	**Applicant's or agent's file reference**		49705		
2	**Applicant**		NOKIA NETWORKS OY, et al.		
12	**Calculation of prescribed fees**		fee amount/multiplier	total amounts (FIM)	
12-1	Transmittal fee	T	⇨	800	
12-2	Search fee	S	⇨	5 618,71	
12-3	International fee Basic fee (first 30 sheets)	b1	2 431,8		
12-4	Remaining sheets		0		
12-5	Additional amount	(X)	53,51		
12-6	Total additional amount	b2	0		
12-7	b1 + b2 =	B	2 431,8		
12-8	Designation fees Number of designations contained in international application		85		
12-9	Number of designation fees payable (maximum 8)		8		
12-10	Amount of designation fee	(X)	523,22		
12-11	Total designation fees	D	4 185,76		
12-12	PCT-EASY fee reduction	R	-749,16		
12-13	Total International fee (B+D-R)	I	⇨	5 868,4	
12-14	Fee for priority document Number of priority documents requested		1		
12-15	Fee per document	(X)	422		
12-16	Total priority document fee	P	⇨	422	
12-17	**TOTAL FEES PAYABLE (T+S+I+P)**		⇨	12 709,11	
12-19	**Mode of payment**		cheque		

VALIDATION LOG AND REMARKS

13-2-6	**Validation messages** **Contents**	Green? Reference number for attached copy of general power of attorney not indicated.

PCT (ANNEX - FEE CALCULATION SHEET) 49705

Original (for **SUBMISSION**) - printed on 25.04.2000 10:40:41 AM

13-2-7	Validation messages Fees	Green? Please verify that modified fee amounts are correct.

PCT

49705

Original (for **SUBMISSION**) - printed on 25.04.2000 10:40:41 AM

PCT-EASY INFORMATION SHEET

(For applicant use only, DO NOT submit this sheet with the international application)

VALIDATION LOG

	Contents
Green?	Reference number for attached copy of general power of attorney not indicated.
	Fees
Green?	Please verify that modified fee amounts are correct.

Before submitting the International Application, please carefully verify that:

-the information contained on printed Request form is correct;
-Box IX of the Request form has been signed;
-all elements of the international application as indicated in Box VIII of the Request form have been attached; and,
-the diskette containing the PCT-EASY zip file of the International Application has been enclosed and has been clearly labeled "PCT-EASY", with the applicant's or agent's file reference, and the first applicant's name.

ATTENTION

DO NOT modify any indications on the Request form printout. The attached PCT-EASY application has been locked. If an error or an omission is discovered at this time, you must copy the submitted application as a template and make the change or correction in a new application (using the submitted application as a template). You may create such a template by copying the submitted application from the "Stored Forms" folder to the "New PCT Forms" folder. Open the new (.0WO) file created in the "New PCT Forms" folder, correct the errors and proceed with the submission process again.

Patent Office

PATENTTI- JA REKISTERIHALLITUS

Patentti- ja innovaatiolinja Patent & Innovation

SEARCH REPORT

TUTKIMUSRAPORTTI

PATENTTIHAKEMUS NRO Appln. No.	**LUOKITUS** Classification
990936	H04L9/00

TUTKITTU AINEISTO Research material

Patenttijulkaisukokoelma (FI, SE, NO, DK, DE, CH, EP, WO, GB, US), tutkitut luokat Published patent specification, researched classes

H04L9, H04K1, H04Q1, G09C1

Tiedonhaut ja muu aineisto Data search and other material

EPODOC, WPI, PAJ

VIITEJULKAISUT Reference publications

Kategoria*) Category	**Julkaisun tunnistetiedot** Identification data	**Koskee vaatimuksia** Relevant to claims
A	US5054066, H04L9/30, Grumman Corporation, palsta 2 rivi 35 - palsta 3 rivi 36, palsta 7 rivit 10 - 50	1, 2, 3, 6, 9 - 11, 13, 15
A	US5345507, H04L9/28, International Business Machines Corporation, palsta 2 rivi 17 - palsta 3 rivi 17, palsta 3 rivi 35 - palsta 7 rivi 44	1 - 3, 5, 6, 9 - 15
A	US5889864, H04L9/00, Plessey Semiconductors Limited, palsta 2 rivit 5 - 43	1-3, 5, 6, 9-15
A	US5694471, H04L9/00, V-ONE Corporation, palsta 3 rivi 25 - palsta 5 rivi 18, palsta 7 rivi 33 - palsta 8 rivi 27	1, 2, 5, 6, 9 - 14
A	EP0840478, H04L9/32, Hitachi, Ltd., sivu 4 rivi 25 - sivu 5 rivi 13	1-3,6,10,11,13

*) X Patentoitavuuden kannalta merkittävä julkaisu yksinään tarkasteltuna
Y Patentoitavuuden kannalta merkittävä julkaisu, kun otetaan huomioon tämä ja yksi tai useampi samaan kategoriaan kuuluva julkaisu
A Yleistä tekniikan tasoa edustava julkaisu, ei kuitenkaan patentoitavuuden este

A) Technological background, not a novelty bar.

Päiväys Date	**Tutkija** Examiner
25.5.2000	Ilpo Tuomi

WO 00/65765
PCT/FI00/00353

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTICE INFORMING THE APPLICANT OF THE COMMUNICATION OF THE INTERNATIONAL APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

To:
BERGGREN OY AB
P.O. Box 16
FIN-00101 Helsinki
FINLANDE

Berggren Oy Ab
10 -11- 2000

Date of mailing (day/month/year) 02 November 2000 (02.11.00)	
Applicant's or agent's file reference 49705 /HL/hm	**IMPORTANT NOTICE**

International application No.	**International filing date** (day/month/year)	**Priority date** (day/month/year)
PCT/FI00/00353	25 April 2000 (25.04.00)	26 April 1999 (26.04.99)

Applicant
NOKIA NETWORKS OY et al

1. Notice is hereby given that the International Bureau has communicated, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this Notice:
   AG,AU,DZ,KP,KR,US

   In accordance with Rule 47.1(c), third sentence, those Offices will accept the present Notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:
   AE,AL,AM,AP,AT,AZ,BA,BB,BG,BR,BY,CA,CH,CN,CR,CU,CZ,DE,DK,DM,EA,EE,EP,ES,FI,GB,GD,
   GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,
   NO,NZ,OA,PL,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TR,TT,TZ,UA,UG,UZ,VN,YU,ZA,ZW
   The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this Notice is a copy of the international application as published by the International Bureau on
   02 November 2000 (02.11.00) under No. WO 00/65765

REMINDER REGARDING CHAPTER II (Article 31(2)(a) and Rule 54.2)

If the applicant wishes to postpone entry into the national phase until 30 months (or later in some Offices) from the priority date, **a demand for international preliminary examination** must be filed with the competent International Preliminary Examining Authority before the expiration of 19 months from the priority date.

It is the applicant's sole responsibility to monitor the 19-month time limit.

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

REMINDER REGARDING ENTRY INTO THE NATIONAL PHASE (Article 22 or 39(1))

If the applicant wishes to proceed with the international application in the **national phase**, he must, within 20 months or 30 months, or later in some Offices, perform the acts referred to therein before each designated or elected Office.

For further important information on the time limits and acts to be performed for entering the national phase, see the Annex to Form PCT/IB/301 (Notification of Receipt of Record Copy) and Volume II of the PCT Applicant's Guide.

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer
J. Zahra

Telephone No. (41-22) 338.83.38

Continuation of Form PCT/IB/

NOTICE INFORMING THE APPLICANT OF THE COMMUNICATION OF THE INTERNATIONAL APPLICATION TO THE DESIGNATED OFFICES

Date of mailing (day/month/year)	**IMPORTANT NOTICE**
02 November 2000 (02.11.00)	
Applicant's or agent's file reference	**International application No.**
49705	PCT/FI00/00353

The applicant is hereby notified that, at the time of establishment of this Notice, the time limit under Rule 46.1 for making amendments under Article 19 has not yet expired and the International Bureau had received neither such amendments nor a declaration that the applicant does not wish to make amendments.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
49705/ML/MM		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/FI00/00353	25/04/2000	26/04/1999
International Patent Classification (IPC) or national classification and IPC H04L9/00		
Applicant NOKIA NETWORKS OY et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 8 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 6 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☒ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
26/11/2000	27.07.2001
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Apostolescu, R Telephone No. +49 89 2399 7950

Form PCT/IPEA/409 (cover sheet) (January 1994)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/FI00/00353

I. Basis of the report

1. With regard to the **elements** of the international application *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17))*:
Description, pages:

1-3,7-11	as originally filed	
4-6	with telefax of	06/07/2001

Claims, No.:

1-17	with telefax of	06/07/2001

Drawings, sheets:

1/4-4/4	as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

   These elements were available or furnished to this Authority in the following language: , which is:

   - ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
   - ☐ the language of publication of the international application (under Rule 48.3(b)).
   - ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

   - ☐ contained in the international application in written form.
   - ☐ filed together with the international application in computer readable form.
   - ☐ furnished subsequently to this Authority in written form.
   - ☐ furnished subsequently to this Authority in computer readable form.
   - ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
   - ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:
- ☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

   (Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-17
	No:	Claims	
Inventive step (IS)	Yes:	Claims	13, 14, 15, 16, 17
	No:	Claims	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12
Industrial applicability (IA)	Yes:	Claims	1-17
	No:	Claims	

2. Citations and explanations
   see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:
see separate sheet

Re Item V

Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

Reference is made to the following documents:

D1: EP 0 564 825 A2 (NOKIA TECHNOLOGY GMBH) 13 October 1993
D2: EP 0 400 234 A1 (M.H. FRANCISCO) 5 December 1990

1. Independent claim 1.

Document D2 (see in particular column 2, line 23 to column 3, line 11; fig. 1), which is considered to represent the most relevant state of the art, discloses, according to the main features of claim 1, a method for checking of data, characterized in that a first reference value is calculated at least partly based on a first authentication value (column 2, line 53 to column 3, line 2).

The subject-matter of claim 1 differs from this disclosure in the calculation of the first reference value.

The problem to be solved by the present invention may therefore be regarded as how to provide an alternative method for calculating the first reference value.

It would be immediately apparent to the person skilled in the art of cryptography that the method known from D2 could be, by some modifications (e. g. combining the authentication value and a error check value with a logical function, said error check value being calculated from the data to be checked) generally known in the art (see document D1, fig. 1), adapted to provide an alternative method for calculating a first reference value.
The skilled person would thus arrive, without the exercise of inventive skill, at a method for checking of data according to claim 1.

The subject-matter of claim 1 does therefore not involve an inventive step (Article 33 (3) PCT).

2. Independent claim 11.

Document D2 (see in particular column 2, line 23 to column 3, line 11; fig. 1) discloses, according to the main features of claim 11, a transmitter that comprises means for deriving an authentication value from the data to be transmitted.

The subject-matter of claim 11 differs from this disclosure in that the transmitter comprises means for deriving an error check value and means for combining the authentication value and said error check value with a logical function for producing a first reference value.

The problem to be solved by the present invention may therefore be regarded as how to provide a transmitter that comprises means for producing a first reference value.

It would be immediately apparent to the person skilled in the art of cryptography that the transmitter known from D2 could be, by some modifications (e. g. including in the transmitter means for deriving an error check value from the data to be transmitted and means for combining the authentication value and said error check value with a logical function) generally known in the art (see document D1, fig. 1), adapted to provide a transmitter that comprises means for producing a reference value.
The skilled person would thus arrive, without the exercise of inventive skill, at a transmitter according to claim 11.

The subject-matter of claim 11 does therefore not involve an inventive step (Article 33 (3) PCT).

The applicant did not put forward any convincing arguments in his replay dated 6.07.01. He only defined in more detail the reference value, the check value and the authentication value used in the claimed method and apparatus invention.
As already argued in the first Written Opinion, these values and how these values are calculated are already known from the prior art documents D1 and D2.

3. Independent claims 13 and 15.

It is considered that independent claims 13 and 15 relate to new and inventive subject-matter (Articles 33 (2) and (3) PCT), since the prior art does not disclose or suggest the specifically claimed receiver for receiving data having means for checking received data according to claim 13 and does not disclose or suggest the specifically claimed station (including the receiver of claim 13) according to claim 15.

Document D1 discloses a method for identifying secret data messages in a transmitting system where a cyclic redundancy check-sum is used for error check. For the CRC-calculation of the secret message a back coupled transfer register is used. When the CRC-value is calculated for the transmitted message, a 16-bit CRC-value is got with a 16-bit coding circuit. The CRC-value is taken to XOR-function together with the unique CRC-identification. The produced CRC-part is added to the end of the message and transmitted to the receiver.
The calculation of an authentication value is already known in the art for example from document D2. A message to be transmitted is introduced in an electronic identification indicia generator. The generator is adapted to generate a first electronic identification indicia that uniquely and selectively identifies the message to be transmitted. Such a generator could generate a selective and unique indicia by the use of a preprogrammed algorithm. The indicia is inserted into the message header and forms a predetermined and readily locatable part of the message passed on to the message transmitter for transmission to a remote location. After receipt of the message by the receiver, a second electronic identification indicia is calculated by an indicia generator using the same algorithm as the generator of the transmitter. A comparator checks if the first and second indicia do match.

The present invention is directed to a receiver (and a transmitter including said receiver) that calculates a second reference value (the first reference value being derived from the received data) and compares this value with a third value from the set of a) the error check value calculated from the received data, b) the authentication value derived for the received data and c) the first reference value.
This specifically claimed receiver and transmitter has the advantage of increasing security in a data transmission system.

4. Dependent claims 3, 4, 5, 7, 8 and 12.

The dependent claims 3, 4, 5, 7, 8 and 12 do not appear to contain any additional features which, in combination with the features of any claim to which they refer, involve an inventive step for the following reasons: the subject-matter of said claims is either directly derivable from the prior art documents D1 and D2 or represent minor design details generally known in the field of communications.

Therefore, the dependent claims 3, 4, 5, 7, 8 and 12 do not meet the requirements of the PCT in respect of inventive step (Articles 33 (3) PCT).

5. Dependent claims 14, 16 and 17.

Dependent claims 14, 16 and 17 contain further details of the receiver of claim 13 and of the transmitter of claim 15 respectively. As they are dependent on claims 13 and 15 respectively, they also satisfy the requirements for novelty and inventive step (Article 33 (2) and (3) PCT).

6. Dependent claims 2, 6, 9 and 10.

The features of dependent claim 2 in combination with the features of claim 1 are not disclosed in their present form in any of the documents cited in the search report.

A new independent claim containing all the features of claims 1 and 2 as presently filed would meet the requirements of Article 33 (3) PCT.

The features of dependent claims 6, 9 and 10 in combination with the features of claim 2 are not disclosed in their present form in any of the documents cited in the search report.
These claims once made dependent on such a new independent claim would also meet the requirements of Article 33 (3) PCT.

Re Item VII

Certain defects in the international application

Contrary to the requirements of Rule 5.1(a)(ii) PCT, the relevant background art disclosed in the documents D1 and D2 is not mentioned in the description, nor are these documents identified therein.

without increasing the packet size. It provides a simple per packet authentication so that the receiver can with one check determine if the packet is valid or not. A second object of the present invention is to provide a transmitter, which is capable of arranging the authentication value into a packet so that the packet size is not increased. A third object of the present invention is to provide a receiver, which is capable of checking, if the transmitted data has changed in the transmission path. A fourth object of the present invention is to provide a mobile station which is capable of transmitting and receiving the authentication value without increasing the packet size.

The above stated objects are achieved by combining the authentication value to the error check data so that it does not add the packet size. Combining the authentication value to error check data is done by using a logical function, for example. At the receiving end the combination of the error check value and the authentication value is processed so that the integrity of the data can be checked.

The advantage of the present invention is that by using this arrangement in a telecommunication system the bandwidth of the system can be saved. It also enables the use of digital signatures with fixed length frames of present protocols without changing the frame formats. As a result, the authenticity can be provided without increasing the packet size. One very important aspect is that the invention is applicable in all digital communication systems.

The method according to the invention is a method for checking data, and it is characterized in that a first reference value is calculated at least partly based on a first error check value calculated from the data and a first authentication value for the data.

The transmitter according to the invention is characterized in that the transmitter comprises

- means for deriving an authentication value from the data to be transmitted,

- means for deriving an error check value from the data to be transmitted and

- means for combining said authentication value and said error check value with a logical function for producing a first reference value.

The receiver for receiving data having means for checking received data according to the invention is characterized in that the receiver comprises

- means for deriving a first reference value from the received data,

- means for calculating a second error check value from the received data,

- means for deriving an authentication value for the received data,

- means for calculating a second reference value at least partly based on a first and a second value from the set of said second error check value, a second authentication value and said first reference value, and

- means for comparing said second reference value with a third value from the set of said second error check value, said second authentication value and said first reference value.

The station, comprising a transmitter and a receiver, according to the invention is characterized in that the transmitter comprises

- means for deriving a first authentication value from the data to be transmitted,

- means for deriving a first error check value from the data to be transmitted, and

- means for combining said first authentication value and said first error check value with a logical function for producing a first reference value

and the receiver comprises

- means for deriving a first reference value from the received data,

- means for calculating a second error check value from the received data,

- means for deriving an authentication value for the received data, this authentication value being a second authentication value,

- means for calculating a second reference value at least partly based on a first and a second value from the set of said second error check value, said second authentication value and said first reference value, and

- means for comparing said second reference value with a third value from the set of said second error check value, said second authentication value and said first reference value.

The present invention will now be described more in detail in the following with the reference to the accompanying drawings, in which

fig. 1 illustrates one possible arrangement of the GPRS network,

fig. 2 illustrates one possible arrangement at the sending end,

fig. 3 illustrates one possible arrangement at the receiving end and

fig. 4 illustrates a block diagram of a mobile station.

In the present invention the data transmitted is processed at the both ends, that is at the sending end and at the receiving end, in the same way so that the integrity of the message can be checked. At the sending end, as shown in figure 2, the error check value, which in this preferred embodiment is a CRC 205, is derived from the original data 201. Next, the authentication value 202, which can be derived for instance by using a packet number or a secret key as an input and a secret algorithm, is combined to the CRC field. The broken line describes that the authentication value 202 is in some way derived from the original data 201. The combination of the CRC 205 and the authentication value 202 is carried out in this preferred embodiment of the invention by using the logical function "exclusive-OR" (XOR) 203. XOR 203 is a function which produces an output of 1 when exactly one of its two inputs is 1. As a result, the data, which is to be sent, comprises the original data field 201 and another field, which consists of the XORed value 308 of the CRC 205 and the authentication value 202. To a man skilled in the art it is obvious that the authentication value 202 can be any value, which is advantageously possible to derive from the original data 201.

At the receiving end the data received is arranged to be processed vice versa, as shown in figure 3. The XORed data 308 is re-XORed 203 with the authentication value 302, which is the same as the authentication value 202 at the sending end in a case where the data sent is not changed. The authentication value 302 can be derived from the received data 301 in the same way as at the sending end. By using the rules of binary algebra the result of this re-XORing 203 is CRC value 304. By comparing 305 this CRC 304 to another CRC 303 calculated at the receiving end from the received data, it can be found, if the data has changed in the transmission path. If the comparison 302 shows that the CRCs 303; 304 are the same, it means that the received data 301 has been transmitted without any changes 306. But, if the comparison 305 shows that the CRCs 303; 304 differ from each other, it means that the original data 201 has changed in the transmission path, or that the authentication value 302 was not correct at the receiving end. As a result, the data received can be erased 306.

AMENDED SHEET

Claims

1. A method for checking of data, **characterized** in that

- a first reference value (204) is calculated (203) at least partly based on a first error check value (205) calculated from the data and a first authentication value (202) for the data.

2. A method according to claim 1, **characterized** in that when checking the data

- a second error check value (303) is calculated from the data,

- a second authentication value (302) is derived for the data,

- a second reference value is calculated at least partly based on a first and a second value from the set of said second error check value, said second authentication value and said first reference value,

- said second reference value is compared (305) with a third value from the set of said second error check value, said second authentication value and said first reference value.

3. A method according to claim 1, **characterized** in that the data is in the form of packets to be sent from a transmitter to a receiver and said first reference value is added to the packet to be sent.

4. A method according to claim 3, **characterized** in that the data is to be sent in a cellular system.

5. A method according to claim 1, **characterized** in that said calculation is performed with the exclusive-OR function.

6. A method according to claim 2, **characterized** in that said first and second authentication values (202; 302) are derived at least partly based on a secret key.

7. A method according to claim 3, **characterized** in that said first authentication value (202) is derived at least partly based on a packet number.

8. A method according to claim 3, **characterized** in that said first authentication value (202) is derived at least partly based on the direction of the packet to be transmitted.

9. A method according to claim 2, **characterized** in that said first and second error check values are CRC values (205; 303; 304).

10. A method according to claim 2, **characterized** in that said first and second authentication values are calculated at least partly based on the data.

11. A transmitter, **characterized** in that the transmitter comprises

- means for deriving an authentication value (202) from the data to be transmitted (201),

- means for deriving an error check value (205) from the data to be transmitted (201) and

- means for combining said authentication value (202) and said error check value (205) with a logical function for producing a first reference value (204).

12. A transmitter according to claim 11, **characterized** in that said logical function is exclusive-OR (203).

13. A receiver for receiving data having means for checking received data, **characterized** in that the receiver comprises

- means for deriving a first reference value (308) from the received data,

- means for calculating an error check value (303) from the received data,

- means for deriving an authentication value (302) for the received data,

- means for calculating a second reference value at least partly based on a first and a second value from the set of said error check value, said authentication value and said first reference value, and

- means for comparing said second reference value with a third value from the set of said error check value, said authentication value and said first reference value.

14. A receiver according to claim 13, **characterized** in that the receiver is arranged to carry out the logical function exclusive-OR (203).

15. A station, comprising a transmitter and a receiver, **characterized** in that the transmitter comprises

- means for deriving a first authentication value (202) from the data to be transmitted (201),

- means for deriving a first error check value (205) from the data to be transmitted (201) and

- means for combining said first authentication value (202) and said first error check value (205) with a logical function for producing a first reference value (204),

and the receiver comprises

- means for deriving a first reference value (308) from the received data,

- means for calculating a second error check value (303) from the received data,

- means for deriving an authentication value (302) for the received data, this authentication value being a second authentication value,

- means for calculating a second reference value at least partly based on a first and a second value from the set of said second error check value, said second authentication value and said first reference value, and

- means for comparing said second reference value with a third value from the set of said second error check value, said second authentication value and said first reference value.

16. A station according to claim 15, **characterized** in that the mobile station (101) is arranged to carry out the logical function exclusive-OR (203).

17. A station according to claims 15 or 16, **characterized** in that the station is a mobile station (101).

PATENT COOPERATION TREATY

From the:
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:
BERGGREN OY AB
P.O. Box 16
00101 Helsinki
FINLANDE

PCT

Berggren Oy Ab
10 -05- 2001
mm | ML

WRITTEN OPINION

(PCT Rule 66) 8/7/04

Date of mailing *(day/month/year)*	08.05.2001
Applicant's or agent's file reference: 49705/ML/MM	**REPLY DUE** **within 2 month(s)** from the above date of mailing

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/FI00/00353	25/04/2000	26/04/1999

International Patent Classification (IPC) or both national classification and IPC
H04L9/00

Applicant
NOKIA NETWORKS OY et al.

1. This written opinion is the **first** drawn up by this International Preliminary Examining Authority.

2. This opinion contains indications relating to the following items:

I	☒	Basis of the opinion
II	☐	Priority
III	☐	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
IV	☐	Lack of unity of invention
V	☒	Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
VI	☐	Certain document cited
VII	☒	Certain defects in the international application
VIII	☒	Certain observations on the international application

3. The applicant is hereby **invited to reply** to this opinion.

When? See the time limit indicated above. The applicant may, before the expiration of that time limit, request this Authority to grant an extension, see Rule 66.2(d).

How? By submitting a written reply, accompanied, where appropriate, by amendments, according to Rule 66.3. For the form and the language of the amendments, see Rules 66.8 and 66.9.

Also: For an additional opportunity to submit amendments, see Rule 66.4. For the examiner's obligation to consider amendments and/or arguments, see Rule 66.4 bis. For an informal communication with the examiner, see Rule 66.6.

If no reply is filed, the international preliminary examination report will be established on the basis of this opinion.

4. The final date by which the international preliminary examination report must be established according to Rule 69.2 is: 26/08/2001.

Name and mailing address of the international preliminary examining authority:
European Patent Office
D-80298 Munich
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Authorized officer / Examiner
Apostolescu, R

Formalities officer (incl. extension of time limits)
Barrio Baranano, A
Telephone No. +49 89 2399 8621

I. Basis of the opinion

1. With regard to the **elements** of the international application (Replacement *sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this opinion as "originally filed"*):

Description, pages:

1-11 as originally filed

Claims, No.:

1-17 as originally filed

Drawings, sheets:

1/4-4/4 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:

☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

   (Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	
Inventive step (IS)	Claims	1, 3, 4, 5, 7, 8, 11, 12
Industrial applicability (IA)	Claims	

2. Citations and explanations
   see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:
see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:
see separate sheet

Re Item V

Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

Reference is made to the following documents:

D1: EP 0 564 825 A2 (NOKIA TECHNOLOGY GMBH) 13 October 1993
D2: EP 0 400 234 A1 (M.H. FRANCISCO) 5 December 1990

1. Independent claim 1.

Document D2 (see in particular column 2, line 23 to column 3, line 11; fig. 1), which is considered to represent the most relevant state of the art, discloses, according to the main features of claim 1, a method for checking of data, characterized in that a first reference value is calculated at least partly based on a first authentication value (column 2, line 53 to column 3, line 2).

The subject-matter of claim 1 differs from this disclosure in the calculation of the first reference value.

The problem to be solved by the present invention may therefore be regarded as how to provide an alternative method for calculating the first reference value.

It would be immediately apparent to the person skilled in the art of cryptography that the method known from D2 could be, by some modifications (e. g. combining the authentication value and a error check value with a logical function, said error check value being calculated from the data to be checked) generally known in the art (see document D1, fig. 1), adapted to provide an alternative method for calculating a first reference value.
The skilled person would thus arrive, without the exercise of inventive skill, at a method for checking of data according to claim 1.

The subject-matter of claim 1 does therefore not involve an inventive step (Article 33 (3) PCT).

2. Independent claim 11.

Document D2 (see in particular column 2, line 23 to column 3, line 11; fig. 1) discloses, according to the main features of claim 11, a transmitter that comprises means for deriving an authentication value from the data to be transmitted.

The subject-matter of claim 11 differs from this disclosure in that the transmitter comprises means for deriving an error check value and means for combining the authentication value and said error check value with a logical function for producing a first reference value.

The problem to be solved by the present invention may therefore be regarded as how to provide a transmitter that comprises means for producing a first reference value.

It would be immediately apparent to the person skilled in the art of cryptography that the transmitter known from D2 could be, by some modifications (e. g. including in the transmitter means for deriving an error check value from the data to be transmitted and means for combining the authentication value and said error check value with a logical function) generally known in the art (see document D1, fig. 1), adapted to provide a transmitter that comprises means for producing a reference value.
The skilled person would thus arrive, without the exercise of inventive skill, at a transmitter according to claim 11.

The subject-matter of claim 11 does therefore not involve an inventive step (Article 33 (3) PCT).

3. Dependent claims 3, 4, 5, 7, 8 and 12.

The dependent claims 3, 4, 5, 7, 8 and 12 do not appear to contain any additional features which, in combination with the features of any claim to which they refer, involve an inventive step for the following reasons: the subject-matter of said claims is either directly derivable from the prior art documents D1 and D2 or represent minor design details generally known in the field of communications.

Therefore, the dependent claims 3, 4, 5, 7, 8 and 12 do not meet the requirements of the PCT in respect of inventive step.

Re Item VII

Certain defects in the international application

1. Contrary to the requirements of Rule 5.1(a)(ii) PCT, the relevant background art disclosed in the documents D1 and D2 is not mentioned in the description, nor are these documents identified therein.

2. All features of the claims must be provided with reference signs placed in parentheses (Rule 6.2(b) PCT).

3. It seems to be an error in the wording of claim 14. The statement "A receiver according to claim 12 ..." should be replaced by the statement "A receiver according to claim 13 ...".

4. It seems to be an error in the wording of claim 12. The statement "A transmitter according to claim 9 ..." should be replaced by the statement "A transmitter according to claim 11 ...".

Re Item VIII

Certain observations on the international application

1. The relative terms "a second error check value" and "a second authentication value" used in the independent claims 13 and 15 have no well-recognised meaning and leaves the reader in doubt as to the meaning of the technical features to which they refers, thereby rendering the definition of the subject-matter of said claims unclear (Article 6 PCT).
A first error check value and a first authentication value have not been used in the independent claims 13 and 15 before.

2. Claims 7 and 8 are dependent on claim 3. The statement used in claims 7 and 8 "said first and second authentication values" is not consistent with the subject-matter of claim 3, where only "a first reference value" is disclosed. Furthermore, claim 3 depend on claim 1, in which only "a first authentication value" is stated.
Therefore, claims 7 and 8 are unclear (Article 6 PCT).

Berggren
PATENTTITOIMISTO • PATENT & TRADEMARK ATTORNEYS

Toimitusjohtaja
Managing Director
J. Nordin*
• PATENTIT,
HYÖDYLLISYYSMALLIT:
• PATENTS,
UTILITY MODELS:
J. Kupiainen*
M. Brax*
E. Heikkinen*
T. Laako*
B. Lassenius*
T. Pelin*
I. Risku*
O-P. Saijonmaa*
J. Svensson*
P. Tanhua*
B. Träskman*
J. Joronen
M. Karttunen
S. Kuisma
M. Laajalahti
V. Tognetty
S. Ylätalo
• MALLIT:
• DESIGNS:
N. Mikander
L. Valjakka
• TAVARAMERKIT,
LAKIASIAT:
• TRADEMARKS,
LEGAL MATTERS:
P. Kolve**
H. Halmetoja**
S. Henn**
I. Karlsson**
E-M. Söderström**
S. Aspola
J. Talvitie

6 July 2001

European Patent Office

D-80298 Munich
Germany

Via facsimile: (8 pages)
999-49 89 2399-4465
CONFIRMATION BY MAIL

U R G E N T!

Our Ref.: 49705/SKU/MM

REPLY TO WRITTEN OPINION
INTERNATIONAL PATENT APPLICATION NO. PCT/FI00/00353
APPLICANT: NOKIA NETWORKS OY
DUE DATE: 8 JULY 2001

In response to the Written Opinion, we respectfully present the following.

A check sum for a piece of data is typically calculated using a known algorithm. Consequently a check sum protects that piece of data from unintentional modifications, such as transmission errors. If the piece of data is modified on purpose, it is possible to recalculate a check sum for the modified piece of data and transmit the modified data onwards with the recalculated check sum. It is known in the field that a check sum may be transmitted together with a corresponding message: both documents D1 and D2, for example, disclose this. Document D2 seems to further disclose a specific method for calculating a check sum. Document D1 further discloses a way to combine information indicating the receiver of the encrypted message to a check sum of an encrypted message.

An authentication value for a piece of data provides typically both data integrity and authenticity of origin (sender). The authenticity of origin is provided typically using secret information, which only the sender (possible also the receiver) is expected to know. The secret information may be, for example, a private key corresponding to a public key of the sender, where said public key is known to the receiver, or a secret key and/or a secret algorithm known to both to the sender and to the receiver. Data integrity is provided typically either using the whole piece of data or a check sum of the piece of data as input for the authentication value. Alternatively, it is possible to ensure integrity and authentication of only a part of the piece of data by using only this part in calculating the authentication value for the piece of data. If either the secret information of the sender is not correct or the protected part of the piece of data is modified on purpose or accidentally, the authentication value reveals this, as it is practically impossible to produce a new authentication value without the secret information. It is also known in the field that an authentication value of a message may be transmitted with the message.

Berggren Oy Ab
Osoite • Address:
PL 16 • P.O.Box 16
FIN-00101 Helsinki
FINLAND
*European Patent Attorney
**European Trademark Attorney

Käyntiosoite • Office:
Graniittitalo
Jaakonkatu 3 A
Helsinki

☎
Nat. 09) 693 701
Int. +358 9 693 701
Fax +358 9 693 3944

email: box@berggren.fi
http: www.berggren.fi

Pankit • Bankers:
NORDEA 157330-15411
SWIFT MRITFIHH
SAMPO 800017-90104
SWIFT PSPBFIHH

Yhtiö • Company:
kr.rek. 80.802
Trade Reg. No. 80.802
Y 0107002-7
VAT FI01070027
Kotipaikka Helsinki

In the claimed invention, a reference value for a data, said reference value then typically sent together with the data, is calculated at least partly based on a check sum and an authentication value. Typically the check sum is calculated using the whole data. The authentication value for the data may be calculated using, together with the actual authentication information, part of the data, the whole data or some information relating to the data.

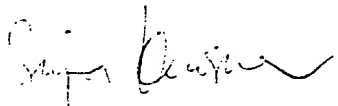
The calculation of the reference value enables the transmission of both a check sum and an authentication value together with a data using the same transmission capacity as in transmitting only the check sum and the data. Furthermore, by transmitting a combination of the check sum and the authentication value (i.e. the reference value) it is possible, for example, to protect parts of the data against accidental modification (i.e. parts protected only by the check sum) and parts of the data against accidental and purposive modifications (i.e. parts protected by the authentication value). In some cases it may be computationally easier to calculate authentication values only for the most significant parts of data than for the whole data. Same flexibility and computational advantages may be achieved by transmitting with a message separately an authentication value and a check sum, but this results in wasted transmission capacity when compared to the claimed invention.

Amended claims, where reference signs are placed where appropriate, are enclosed. Claim 1 now specifies an authentication value for the data. Claims 3-6, and 9-11 are original. Claims 12, 14, 16 and 17 now refer to correct claims, otherwise they are original. Claim 2 now mentions that a second authentication value is derived; support for this modification is on page 6, rows 23-24 of the description. Reference to second authentication value is removed from Claims 7 and 8. Claims 13 and 15 mention means for deriving an authentication value for the received data. In Claim 15, terms first and second authentication/error check value are now used consistently.

The description is brought into conformity with the amended claims. Replacement pages 4, 5 and 6 are enclosed.

A reconsideration of the arguments presented in the Written Opinion regarding the novelty and inventiveness of the claimed invention is respectfully requested.

BERGGREN OY AB



Sirpa Kuisma
Patent Attorney

without increasing the packet size. It provides a simple per packet authentication so that the receiver can with one check determine if the packet is valid or not. A second object of the present invention is to provide a transmitter, which is capable of arranging the authentication value into a packet so that the packet size is not increased. A third object of the present invention is to provide a receiver, which is capable of checking, if the transmitted data has changed in the transmission path. A fourth object of the present invention is to provide a mobile station which is capable of transmitting and receiving the authentication value without increasing the packet size.

The above stated objects are achieved by combining the authentication value to the error check data so that it does not add the packet size. Combining the authentication value to error check data is done by using a logical function, for example. At the receiving end the combination of the error check value and the authentication value is processed so that the integrity of the data can be checked.

The advantage of the present invention is that by using this arrangement in a telecommunication system the bandwidth of the system can be saved. It also enables the use of digital signatures with fixed length frames of present protocols without changing the frame formats. As a result, the authenticity can be provided without increasing the packet size. One very important aspect is that the invention is applicable in all digital communication systems.

The method according to the invention is a method for checking data, and it is characterized in that a first reference value is calculated at least partly based on a first error check value calculated from the data and a first authentication value for the data.

The transmitter according to the invention is characterized in that the transmitter comprises

- means for deriving an authentication value from the data to be transmitted,

- means for deriving an error check value from the data to be transmitted and

- means for combining said authentication value and said error check value with a logical function for producing a first reference value.

The receiver for receiving data having means for checking received data according to the invention is characterized in that the receiver comprises

- means for deriving a first reference value from the received data,

- means for calculating a second error check value from the received data,

- means for deriving an authentication value for the received data,

- means for calculating a second reference value at least partly based on a first and a second value from the set of said second error check value, a second authentication value and said first reference value, and

- means for comparing said second reference value with a third value from the set of said second error check value, said second authentication value and said first reference value.

The station, comprising a transmitter and a receiver, according to the invention is characterized in that the transmitter comprises

- means for deriving a first authentication value from the data to be transmitted,

- means for deriving a first error check value from the data to be transmitted, and

- means for combining said first authentication value and said first error check value with a logical function for producing a first reference value

and the receiver comprises

- means for deriving a first reference value from the received data,

- means for calculating a second error check value from the received data,

- means for deriving an authentication value for the received data, this authentication value being a second authentication value,

- means for calculating a second reference value at least partly based on a first and a second value from the set of said second error check value, said second authentication value and said first reference value, and

- means for comparing said second reference value with a third value from the set of said second error check value, said second authentication value and said first reference value.

The present invention will now be described more in detail in the following with the reference to the accompanying drawings, in which

fig. 1 illustrates one possible arrangement of the GPRS network,

fig. 2 illustrates one possible arrangement at the sending end,

fig. 3 illustrates one possible arrangement at the receiving end and

fig. 4 illustrates a block diagram of a mobile station.

In the present invention the data transmitted is processed at the both ends, that is at the sending end and at the receiving end, in the same way so that the integrity of the message can be checked. At the sending end, as shown in figure 2, the error check value, which in this preferred embodiment is a CRC 205, is derived from the original data 201. Next, the authentication value 202, which can be derived for instance by using a packet number or a secret key as an input and a secret algorithm, is combined to the CRC field. The broken line describes that the authentication value 202 is in some way derived from the original data 201. The combination of the CRC 205 and the authentication value 202 is carried out in this preferred embodiment of the invention by using the logical function "exclusive-OR" (XOR) 203. XOR 203 is a function which produces an output of 1 when exactly one of its two inputs is 1. As a result, the data, which is to be sent, comprises the original data field 201 and another field, which consists of the XORed value 308 of the CRC 205 and the authentication value 202. To a man skilled in the art it is obvious that the authentication value 202 can be any value, which is advantageously possible to derive from the original data 201.

At the receiving end the data received is arranged to be processed vice versa, as shown in figure 3. The XORed data 308 is re-XORed 203 with the authentication value 302, which is the same as the authentication value 202 at the sending end in a case where the data sent is not changed. The authentication value 302 can be derived from the received data 301 in the same way as at the sending end. By using the rules of binary algebra the result of this re-XORing 203 is CRC value 304. By comparing 305 this CRC 304 to another CRC 303 calculated at the receiving end from the received data, it can be found, if the data has changed in the transmission path. If the comparison 302 shows that the CRCs 303; 304 are the same, it means that the received data 301 has been transmitted without any changes 306. But, if the comparison 305 shows that the CRCs 303; 304 differ from each other, it means that the original data 201 has changed in the transmission path, or that the authentication value 302 was not correct at the receiving end. As a result, the data received can be erased 306.

Claims

1. A method for checking of data, **characterized** in that

- a first reference value (204) is calculated (203) at least partly based on a first error check value (205) calculated from the data and a first authentication value (202) for the data.

2. A method according to claim 1, **characterized** in that when checking the data

- a second error check value (303) is calculated from the data,

- a second authentication value (302) is derived for the data,

- a second reference value is calculated at least partly based on a first and a second value from the set of said second error check value, said second authentication value and said first reference value,

- said second reference value is compared (305) with a third value from the set of said second error check value, said second authentication value and said first reference value.

3. A method according to claim 1, **characterized** in that the data is in the form of packets to be sent from a transmitter to a receiver and said first reference value is added to the packet to be sent.

4. A method according to claim 3, **characterized** in that the data is to be sent in a cellular system.

5. A method according to claim 1, **characterized** in that said calculation is performed with the exclusive-OR function.

6. A method according to claim 2, **characterized** in that said first and second authentication values (202; 302) are derived at least partly based on a secret key.

7. A method according to claim 3, **characterized** in that said first authentication value (202) is derived at least partly based on a packet number.

8. A method according to claim 3, **characterized** in that said first authentication value (202) is derived at least partly based on the direction of the packet to be transmitted.

9. A method according to claim 2, **characterized** in that said first and second error check values are CRC values (205; 303; 304).

10. A method according to claim 2, **characterized** in that said first and second authentication values are calculated at least partly based on the data.

11. A transmitter, **characterized** in that the transmitter comprises

- means for deriving an authentication value (202) from the data to be transmitted (201),

- means for deriving an error check value (205) from the data to be transmitted (201) and

- means for combining said authentication value (202) and said error check value (205) with a logical function for producing a first reference value (204).

12. A transmitter according to claim 11, **characterized** in that said logical function is exclusive-OR (203).

13. A receiver for receiving data having means for checking received data, **characterized** in that the receiver comprises

- means for deriving a first reference value (308) from the received data,

- means for calculating an error check value (303) from the received data,

- means for deriving an authentication value (302) for the received data,

- means for calculating a second reference value at least partly based on a first and a second value from the set of said error check value, said authentication value and said first reference value, and

- means for comparing said second reference value with a third value from the set of said error check value, said authentication value and said first reference value.

14. A receiver according to claim 13, **characterized** in that the receiver is arranged to carry out the logical function exclusive-OR (203).

15. A station, comprising a transmitter and a receiver, **characterized** in that the transmitter comprises

- means for deriving a first authentication value (202) from the data to be transmitted (201),

- means for deriving a first error check value (205) from the data to be transmitted (201) and

- means for combining said first authentication value (202) and said first error check value (205) with a logical function for producing a first reference value (204),

and the receiver comprises

- means for deriving a first reference value (308) from the received data,

- means for calculating a second error check value (303) from the received data,

- means for deriving an authentication value (302) for the received data, this authentication value being a second authentication value,

- means for calculating a second reference value at least partly based on a first and a second value from the set of said second error check value, said second authentication value and said first reference value, and

- means for comparing said second reference value with a third value from the set of said second error check value, said second authentication value and said first reference value.

16. A station according to claim 15, **characterized** in that the mobile station (101) is arranged to carry out the logical function exclusive-OR (203).

17. A station according to claims 15 or 16, **characterized** in that the station is a mobile station (101).